528,205

(12)特許協力条約に基づいて公開された国際出

2005

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004 年4 月8 日 (08.04.2004)

PCT

(10) 国際公開番号
WO 2004/029819 A1

(51) 国際特許分類[7]: G06F 15/00, H04B 7/26, H04L 12/28

(21) 国際出願番号: PCT/JP2003/012318

(22) 国際出願日: 2003 年9 月26 日 (26.09.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-284334 2002 年9 月27 日 (27.09.2002) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真１００６番地 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 田中 武志 (TANAKA,Takeshi) [JP/JP]; 〒239-0847 神奈川県 横須賀市 光の丘６−２−４０６ Kanagawa (JP). 荒牧 隆 (ARAMAKI,Takashi) [JP/JP]; 〒232-0061 神奈川県 横浜市 南区大岡１−３５−１０ Kanagawa (JP). 平野 純 (HIRANO,Jun) [JP/JP]; 〒239-0843 神奈川県 横須賀市 津久井３−２０−９−２０６ Kanagawa (JP).

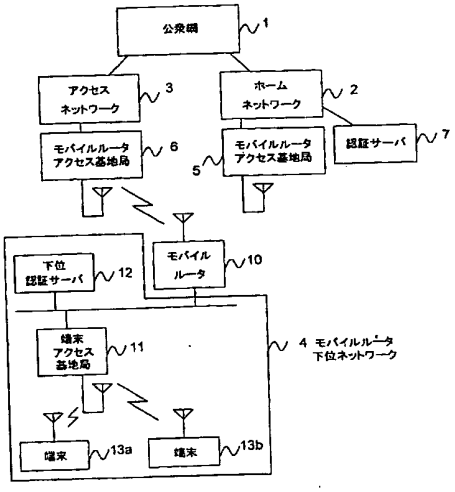
(74) 代理人: 二瓶 正敬 (NIHEI,Masayuki); 〒160-0004 東京都 新宿区 四谷２丁目１２−５ 第６冨沢ビル６Ｆ Tokyo (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG,

[続葉有]

(54) Title: TERMINAL AUTHENTICATION SYSTEM, TERMINAL AUTHENTICATION METHOD, AND TERMINAL AUTHENTICATION SERVER

(54) 発明の名称: 端末認証システム及び端末認証方法並びに端末認証サーバ



1...PUBLIC NETWORK
3...ACCESS NETWORK
6...MOBILE ROUTER ACCESS BASE STATION
2...HOME NETWORK
5...MOBILE ROUTER ACCESS BASE STATION
7...AUTHENTICATION SERVER
12...LOWER NODE AUTHENTICATION SERVER
10...MOBILE ROUTER
11...TERMINAL ACCESS BASE STATION
13a...TERMINAL
13b...TERMINAL
4...MOBILE ROUTER LOWER NODE NETWORK

(57) Abstract: It is possible to effectively authenticate a terminal which attempts connection to (participation in) a mobile network even when the connection between a mobile router and a ground side mobile router access base station is unstable or disabled. In addition to a first authentication server (authentication server (7)) arranged at a position apart from a mobile network (mobile router lower node network (4)) arranged in a mobile body, a second authentication server (lower node authentication server (12)) is arranged in the mobile network so that authentication of mobile terminals (terminals 13a, 13b) can also be performed in the second authentication server. Especially when the connection between the mobile network of the mobile body side and the first authentication server of the ground side (that is, communication between a mobile router 10 and mobile router access base stations 5, 6) is disabled, the second authentication server authenticates a mobile terminal which attempts to participate in the mobile network.

(57) 要約: 移動するモバイルルータと地上側のモバイルルータアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことを目的とし、移動体内に配置されている移動ネットワーク（モバイルルータ下位ネットワーク４）から離れた場所に配置された第１認証サーバ（認証サーバ７）とは別に、第２認証サーバ（下位認証サーバ１２）を移動ネットワーク内に配置し、第２認証サーバにおいても移動端末（端末１３ａ、１３ｂ）の認証が行えるようにする。特に、移動体側の移動ネットワークと地上側の第１認証サーバとの間の接続（すなわち、モバイルルータ１０とモバイルルータアクセス基地局５、６間との通信）が不可能となった場合に、第２認証サーバが、移動ネットワークへの参加を試みる移動端末の認証を行うようにする。

WO 2004/029819 A1

SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

端末認証システム及び端末認証方法並びに端末認証サーバ

技術分野

本発明は、移動体内に配置されている移動ネットワークに移動端末が参加する際に認証処理を行う端末認証システム及び端末認証方法並びに端末認証サーバに関する。

背景技術

従来、端末がモバイルルータ下位ネットワーク（移動体内に配置される移動ネットワーク）への接続（参加）を行おうとする場合、その端末の接続の可否を決める認証処理は、移動可能なモバイルルータ下位ネットワークとは異なる地上側のホームネットワークに属する認証サーバで行われている。認証サーバ７は、端末から利用者名やパスワードなどの認証に必要となる認証データを受け、この認証データを参照し、当該端末に対して、モバイルルータ下位ネットワークへの接続の許可／不許可を決定する認証処理を行っている。

また、例えば、（特許文献１）には、所定の端末の認証情報を有するＬＡＮ（Local Area Network：ローカルエリアネットワーク）とは異なるＬＡＮに当該所定の端末が接続しようとした場合、所定の端末が接続を試みているＬＡＮの認証サーバが、所定の端末の認証情報を有するＬＡＮの認証サーバに対して、所定の端末の認証を依頼し、所定の端末がＬＡＮに接続する権利を有しているか否かを判断する方法が開示されている。

特許文献１　　特開平１０－７０５４０号公報（段落［００１４］～［

００６７］、図１、図２、図５）

しかしながら、モバイルルータは移動可能であり、かつ、アクセス基地局と無線通信によって接続する。したがって、モバイルルータとアクセス基地局との間の接続は不安定であり、一時的に接続が利用できなくなってしまうことが頻繁に起きる。このように、接続が利用不可能となってしまった状態では、モバイルルータ下位ネットワーク（移動ネットワーク）は、ホームネットワーク上の認証サーバに対して、端末の認証を依頼することができず、端末の認証は不可能となってしまう。したがって、モバイルルータ下位ネットワークへの接続を試みている端末は、モバイルルータがアクセス基地局と接続できるようになるまでの間、モバイルルータ下位ネットワークへの接続（参加）ができないという問題がある。また、モバイルルータ下位ネットワークが移動し、ホームネットワークから離れた場合には、モバイルルータ下位ネットワークとホームネットワーク上の認証サーバとの距離は広がり、認証における時間やトラフィックなどが増大してしまうという問題がある。

発明の開示

上記課題を解決するため、本発明では、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、モバイルルータ下位ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことを可能とする端末認証システム及び端末認証方法並びに端末認証サーバを提供することを目的とする。

上記目的を達成するため、本発明の端末認証システムでは、移動体内に配置されている移動ネットワーク（モバイルルータ下位ネットワーク）から離れた場所に配置された第１認証サーバ（認証サーバ）とは別に、第２認証サーバ（下位認証サーバ）を移動ネットワーク内に配置し、第

2認証サーバにおいても移動端末（端末）の認証が行えるよう構成されている。

この構成により、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことが可能となる。

さらに、本発明の端末認証システムでは、第2認証サーバが、移動端末の認証を行うことを可能とする認証手段と、移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有している。

この構成により、移動ネットワークに属し、移動体と共に移動する第2認証サーバで確実に認証処理を行うことが可能となる。

さらに、本発明の端末認証システムでは、移動端末から第2認証サーバに対して、認証要求が送信されるよう構成されている。

この構成により、第2認証サーバが、移動ネットワークへの参加を試みている移動端末の存在を確実に認識できるようになる。

さらに、本発明の端末認証システムでは、第2認証サーバが、第1認証サーバと第2認証サーバとの通信が可能か否かを判断する接続判断手段を有し、第2認証サーバが移動端末から認証要求を受けた場合、第1認証サーバとの通信が可能と判断された場合には第1認証サーバに認証要求を送って第1認証サーバから移動端末の認証結果を受信し、第1認証サーバとの通信が不可能と判断された場合には認証手段を用いて移動端末の認証を行うよう構成されている。

この構成により、第1認証サーバにおける認証が可能な場合には、第1認証サーバで認証を行い、第1認証サーバでの認証が不可能な場合のみ、第2認証サーバで認証を行うようにすることが可能となる。

さらに、本発明の端末認証システムでは、第1認証サーバに認証要求を送って第1認証サーバから移動端末の認証結果を受信した場合、第2

認証サーバは、移動端末の識別情報と移動端末の認証結果とを関連付けて、情報格納手段に認証データとして格納するよう構成されている。

この構成により、第２認証サーバは、第１認証サーバで認証に成功した移動端末を把握することが可能となり、次回以降、当該移動端末の認証を第２認証サーバで行えるようになる。

さらに、本発明の端末認証システムでは、第２認証サーバが、第１認証サーバと第２認証サーバとの通信が可能か否かを判断する接続判断手段を有し、接続判断手段が第１認証サーバとの通信が可能か否かを判断し、第１認証サーバとの通信が可能と判断された場合、第２認証サーバは、任意のタイミングで第１認証サーバから移動端末の認証に必要となる認証データを取得し、情報格納手段に格納するよう構成されている。

この構成により、第２認証サーバは、第１認証サーバとの通信が可能な状態のときに、端末の認証に必要な情報をあらかじめ第１認証サーバから取得できるようになる。

さらに、本発明の端末認証システムでは、第２認証サーバは、所定のタイミングで第１認証サーバから認証データを取得し、情報格納手段に格納されている認証データを更新するよう構成されている。

この構成により、第２認証サーバは、第１認証サーバとの同期を図ることが可能となり、第２認証サーバは、常に第１認証サーバが格納する最新の情報を取得することが可能となる。

さらに、本発明の端末認証システムでは、第２認証サーバで移動端末の認証を行って移動端末の認証に失敗した場合、第２認証サーバは、第１認証サーバに認証要求を送って第１認証サーバから移動端末の認証結果を受信するよう構成されている。

この構成により、なるべく第２認証サーバで認証を行い、認証に失敗した場合のみ第１認証サーバで、確実な認証処理を再度行うことによっ

て、時間やトラフィックの削減を図ることが可能となる。

さらに、本発明の端末認証システムでは、第２認証サーバから認証要求を送信した移動端末に対して、第１認証サーバ又は第２認証サーバで行われた認証結果が通知されるよう構成されている。

この構成により、第１認証サーバ又は第２認証サーバで行われた認証結果が、第２認証サーバから移動端末に対して通知されるようにすることが可能となり、第２認証サーバが、すべての端末の認証結果を把握できるようになる。

また、上記目的を達成するため、本発明の端末認証方法では、移動体内に配置されている移動ネットワークに移動端末が参加する場合、移動ネットワークから離れた場所に配置された第１認証サーバとは別に、移動ネットワーク内に配置された第２認証サーバが、移動端末の認証を行うようにしている。

これにより、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことが可能となる。

さらに、本発明の端末認証方法では、移動端末が、第２認証サーバに対して、認証要求を送信するようにしている。

これにより、第２認証サーバが、移動ネットワークへの参加を試みている移動端末の存在を確実に認識できるようになる。

さらに、本発明の端末認証方法では、第２認証サーバが移動端末から認証要求を受けた場合、第１認証サーバと第２認証サーバとの通信が可能か否かを判断し、第１認証サーバとの通信が可能と判断された場合には第１認証サーバに認証要求を送って第１認証サーバから移動端末の認証結果を受信し、第１認証サーバとの通信が不可能と判断された場合には第２認証サーバが移動端末の認証を行うようにしている。

これにより、第１認証サーバにおける認証が可能な場合には、第１認証サーバで認証を行い、第１認証サーバでの認証が不可能な場合のみ、第２認証サーバで認証を行うようにすることが可能となる。

さらに、本発明の端末認証方法では、第１認証サーバに認証要求を送って第１認証サーバから移動端末の認証結果を受信した場合、第２認証サーバは、移動端末の識別情報と移動端末の認証結果とを関連付けて格納するようにしている。

これにより、第２認証サーバは、第１認証サーバで認証に成功した移動端末を把握することが可能となり、次回以降、当該移動端末の認証を第２認証サーバで行えるようになる。

さらに、本発明の端末認証方法では、第２認証サーバが、第１認証サーバと第２認証サーバとの通信が可能か否かを判断し、第１認証サーバとの通信が可能と判断された場合には、任意のタイミングで第１認証サーバから移動端末の認証に必要となる認証データを取得し格納するようにしている。

これにより、第２認証サーバは、第１認証サーバとの通信が可能な状態のときに、端末の認証に必要な情報をあらかじめ第１認証サーバから取得できるようになる。

さらに、本発明の端末認証方法では、第２認証サーバが、所定のタイミングで第１認証サーバから認証データを取得し、第２認証サーバに格納されている認証データを更新するようにしている。

これにより、第１認証サーバで、確実な認証処理を再度行うことによって、時間やトラフィックの削減を図ることが可能となる。

さらに、本発明の端末認証方法では、第２認証サーバが、認証要求を送信した移動端末に対して、第１認証サーバ又は第２認証サーバで行われた認証結果を通知するようにしている。

これにより、第１認証サーバ又は第２認証サーバで行われた認証結果が、第２認証サーバから移動端末に対して通知されるようにすることが可能となり、第２認証サーバが、すべての端末の認証結果を把握できるようになる。

また、上記目的を達成するため、本発明の端末認証サーバは、移動体内に配置されている移動ネットワークに移動端末が参加する場合、移動端末の認証を行うことが可能な端末認証サーバであり、移動ネットワークから離れた場所に配置された端末認証サーバとは別に、移動ネットワーク内に配置されるよう構成されている。

この構成により、移動するモバイルルータと地上側のアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続（参加）を試みている端末の認証を効率良く行うことが可能となる。

さらに、本発明の端末認証サーバでは、移動端末の認証を行うことを可能とする認証手段と、移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有している。

この構成により、移動ネットワークに属し、移動体と共に移動する端末認証サーバで確実に認証処理を行うことが可能となる。

さらに、本発明の端末認証サーバでは、移動端末から認証要求を受信するよう構成されている。

この構成により、移動ネットワーク内の端末認証サーバが、移動ネットワークへの参加を試みている移動端末の存在を確実に認識できるようになる。

さらに、本発明の端末認証サーバでは、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続判断手段を有し、移動端末から認証要求を受けた場合、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断さ

れた場合には、移動ネットワークから離れた場所に配置された端末認証サーバに認証要求を送って、移動ネットワークから離れた場所に配置された端末認証サーバから移動端末の認証結果を受信し、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が不可能と判断された場合には、認証手段を用いて移動端末の認証を行うよう構成されている。

この構成により、ホームネットワークに属する端末認証サーバにおける認証が可能な場合には、ホームネットワークに属する端末認証サーバで認証を行い、ホームネットワークに属する端末認証サーバでの認証が不可能な場合のみ、移動ネットワーク内の端末認証サーバで認証を行うようにすることが可能となる。

さらに、本発明の端末認証サーバでは、移動ネットワークから離れた場所に配置された端末認証サーバから移動端末の認証結果を受信した場合、移動端末の識別情報と移動端末の認証結果とを関連付けて、情報格納手段に認証データとして格納するよう構成されている。

この構成により、移動ネットワーク内の端末認証サーバは、ホームネットワークに属する端末認証サーバで認証に成功した移動端末を把握することが可能となり、次回以降、当該移動端末の認証を移動ネットワーク内の端末認証サーバで行えるようになる。

さらに、本発明の端末認証サーバでは、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続判断手段を有し、移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断された場合、任意のタイミングで、移動ネットワークから離れた場所に配置された端末認証サーバから移動端末の認証に必要となる認証データを取得し、情報格納手段に格納する構成されている。

この構成により、移動ネットワーク内の端末認証サーバは、ホームネットワークに属する端末認証サーバとの通信が可能な状態のときに、端末の認証に必要な情報をあらかじめホームネットワークに属する端末認証サーバから取得できるようになる。

さらに、本発明の端末認証サーバでは、所定のタイミングで、移動ネットワークから離れた場所に配置された端末認証サーバから認証データを取得し、情報格納手段に格納されている前記認証データを更新するよう構成されている。

この構成により、移動ネットワーク内の端末認証サーバは、ホームネットワークに属する端末認証サーバとの同期を図ることが可能となり、移動ネットワーク内の端末認証サーバは、常にホームネットワークに属する端末認証サーバが格納する最新の情報を取得することが可能となる。

さらに、本発明の端末認証サーバでは、認証手段により移動端末の認証を行って、移動端末の認証に失敗した場合、移動ネットワークから離れた場所に配置された端末認証サーバに認証要求を送って端末認証サーバから移動端末の認証結果を受信するよう構成されている。

この構成により、なるべく移動ネットワーク内の端末認証サーバで認証を行い、認証に失敗した場合のみホームネットワークに属する端末認証サーバで、確実な認証処理を再度行うことによって、時間やトラフィックの削減を図ることが可能となる。

さらに、本発明の端末認証サーバでは、認証要求を送信した移動端末に対して、移動ネットワークから離れた場所に配置された端末認証サーバ、又は、当該端末認証サーバで行われた認証結果を通知するよう構成されている。

この構成により、ホームネットワークに属する端末認証サーバ又は移動ネットワーク内の端末認証サーバで行われた認証結果が、移動ネット

ワーク内の端末認証サーバから移動端末に対して通知されるようにすることが可能となり、移動ネットワーク内の端末認証サーバが、すべての端末の認証結果を把握できるようになる。

図面の簡単な説明

図１は、本発明の実施の形態を示すネットワーク構成図、

図２は、本発明の実施の形態のネットワークに配置されている端末の内部構成を示すブロック図、

図３は、本発明の実施の形態のネットワークに配置されているモバイルルータの内部構成を示すブロック図、

図４は、本発明の実施の形態のネットワークに配置されている下位認証サーバの内部構成を示すブロック図、

図５は、図４に示す下位認証サーバの動作を説明するためのフローチャート、

図６は、本発明の実施の形態のネットワークに配置されている下位認証サーバの内部構成の別の一例を示すブロック図である。

発明を実施するための最良の形態

以下、図面を参照しながら、本発明の実施の形態について説明する。図１は、本発明の実施の形態を示すネットワーク構成図である。図１に示すネットワークは、公衆網１、ホームネットワーク２、アクセスネットワーク３、モバイルルータ下位ネットワーク４、ホームネットワーク２と接続するモバイルルータアクセス基地局５、アクセスネットワーク３と接続するモバイルルータアクセス基地局６、ホームネットワーク２に接続する認証サーバ７、モバイルルータ下位ネットワーク４と接続するモバイルルータ１０により構成される。

モバイルルータ下位ネットワーク４は、例えば、移動可能な乗り物などの移動体内に配置されているものであり、モバイルルータ１０を介してモバイルルータアクセス基地局５、６と無線通信による接続が可能である。すなわち、モバイルルータ１０とモバイルルータアクセス基地局５とが無線通信によって接続している場合には、モバイルルータ下位ネットワーク４は、モバイルルータ１０、モバイルルータアクセス基地局５、ホームネットワーク２を経由して、公衆網１と接続可能とであり、モバイルルータ１０とモバイルルータアクセス基地局６とが無線通信によって接続している場合には、モバイルルータ下位ネットワーク４は、モバイルルータ１０、モバイルルータアクセス基地局６、アクセスネットワーク３を経由して、公衆網１と接続可能である。なお、図１において、アクセスネットワーク３、モバイルルータアクセス基地局５、６はそれぞれ１つずつ図示されているが、複数配置することも可能である。

また、モバイルルータ下位ネットワーク４は、端末アクセス基地局１１、モバイルルータ下位ネットワーク４上の下位認証サーバ１２、複数の端末１３（図１では、端末１３ａ、１３ｂの２つの端末１３が図示されている）により構成されている。端末アクセス基地局１１、モバイルルータ下位ネットワーク４上の下位認証サーバ１２は、モバイルルータ１０と接続されており、また、端末１３は、端末アクセス基地局１１との無線通信を介して、モバイルルータ１０や下位認証サーバ１２への接続が可能であり、さらには、モバイルルータ１０からホームネットワーク２やアクセスネットワーク３を経由して、公衆網１への接続が可能である。

モバイルルータ１０及びモバイルルータ下位ネットワーク４は、本来ホームネットワーク２に所属し、管理されており、端末１３がモバイルルータ下位ネットワーク４に接続する権利を有するか否かの確認（認証

）は、認証サーバ７によって行われる。また、認証サーバ７には、この認証処理を行うための認証データ（利用者名やパスワードなど）が格納されている。

次に、図１に示す端末１３の内部構成の一例について説明する。図２は、本発明の実施の形態のネットワークに配置されている端末の内部構成を示すブロック図である。なお、図１に示されている端末１３は、図２に示す内部構成を有している。図２に示す端末１３は、無線通信手段２０、通信制御手段２１、送信手段２２、受信手段２３、情報格納手段２４、入出力制御手段２５、入出力手段２６により構成される。

無線通信手段２０及び通信制御手段２１は、端末アクセス基地局１１などの端末１３外部の通信装置との通信を行うことを可能とするものである。無線通信手段２０がデータを受信した場合、その受信データは、通信制御手段２１を経由して受信手段２３に供給され、さらに、受信データは、受信手段２３から情報格納手段２４や入出力制御手段２５に供給可能なようになっている。また、情報格納手段２４には、ＭＡＣアドレスなどの端末ＩＤや認証データが格納されており、例えば、認証サーバ７や下位認証サーバ１２に認証要求を送信する場合、送信手段２２は、通信制御手段２１及び無線通信手段２０を通じて、これらの端末ＩＤや認証データを外部に送信することが可能である。また、入出力制御手段２５及び入出力手段２６は、入力データの送信や受信データの出力を可能とするものであり、認証に成功して、端末１３がモバイルルータ下位ネットワーク４に接続可能となった場合には、主に、入出力制御手段２５及び入出力手段２６を介して、通信データの送受信が行われる。

次に、図１に示すモバイルルータ１０の内部構成の一例について説明する。図３は、本発明の実施の形態のネットワークに配置されているモバイルルータの内部構成を示すブロック図である。なお、図１に示され

ているモバイルルータ１０は、図３に示す内部構成を有している。図３に示すモバイルルータ１０は、ローカル通信手段３１、ローカル通信制御手段３２、外部接続検知結果送信手段３３、外部接続検知手段３４、通信制御手段３５、無線通信手段３６、経路制御手段３７により構成される。

無線通信手段３６及び通信制御手段３５は、モバイルルータアクセス基地局５、６などのモバイルルータ１０外部の通信装置との通信を行うことを可能とするものである。また、外部接続検知手段３４は、無線通信手段３６がモバイルルータ１０外部との無線接続が利用可能かを検知し、その外部接続検知結果を経路制御手段３７及び外部接続検知結果送信手段３３に伝達するものである。

外部接続検知結果送信手段３３は、ローカル通信制御手段３２を介してローカル通信手段３１と接続し、外部接続検知結果をＬＡＮ３０上に出力する。このＬＡＮ３０には、端末アクセス基地局１１や下位認証サーバ１２が接続しており、外部接続検知結果送信手段３３から下位認証サーバ１２に対して、外部接続検知結果を伝達することが可能である。

また、ローカル通信制御手段３２は、ローカル通信手段３１を介して、ＬＡＮ３０に接続する端末アクセス基地局１１や下位認証サーバ１２、さらには、端末アクセス基地局１１に接続する端末１３から、モバイルルータ下位ネットワーク４外部への送信データを受信することが可能である。経路制御手段３７は、ローカル通信制御手段３２が受信した当該送信データに対して適切に経路制御を行い、経路制御された当該送信データは、通信制御手段３５及び無線通信手段３６を介してモバイルルータ１０外部の通信装置に無線通信によって伝送される。また、無線通信手段３６及び通信制御手段３５を介してモバイルルータ下位ネットワーク４外部から受信した受信データに関しても、同様に経路制御手段３７

が適切に経路制御を行い、ローカル通信制御手段３２及びローカル通信手段３１を介してＬＡＮ３０上に伝送される。

次に、図１に示す下位認証サーバ１２の内部構成の一例について説明する。図４は、本発明の実施の形態のネットワークに配置されている下位認証サーバの内部構成を示すブロック図である。なお、図１に示されている下位認証サーバ１２は、図４に示す内部構成を有している。図４に示す下位認証サーバ１２は、ローカル通信手段４１、ローカル通信制御手段４２、外部接続検知結果受信手段４３、認証要求受付手段４４、認証依頼送信手段４５、認証結果受信手段４６、認証結果送信手段４７、認証データ比較手段４８、情報格納手段４９により構成される。

また、図５は、図４に示す下位認証サーバの動作を説明するためのフローチャートである。以下、図５を参照しながら下位認証サーバ１２の動作について説明する。まず、下位認証サーバ１２は、移動ネットワークに参加しようとしている端末１３から、当該端末１３の端末ＩＤ及びこの端末１３の利用者名とパスワードを含む認証データを認証要求として受信する（ステップＳ２）。一方で、下位認証サーバ１２は、ＬＡＮ３０を経由してモバイルルータ１０から送信されてくる外部接続検知結果を、ローカル通信手段４１及びローカル通信制御手段４２を介して、外部接続検知結果受信手段４３により受信する（ステップＳ３）。なお、下位認証サーバ１２は、端末１３から認証要求を受けた場合にのみ、モバイルルータ１０に対して外部接続検知結果を要求するようにすることも可能であり、また、定期的にモバイルルータ１０から外部接続検知結果の取得を行うようにすることも可能である。

外部接続検知結果受信手段４３によって受信された外部接続検知結果は、認証要求受付手段４４に供給され、外部接続が利用可能か否か（すなわち、認証サーバ７との通信が可能か否か）が判断される（ステップ

Ｓ４）。外部接続が利用可能な場合には、認証要求と共に端末１３から受信した認証データを情報格納手段４９内の「利用者の認証データ」テーブルに格納し（ステップＳ５）、認証要求受付手段４４から認証依頼送信手段４５に認証要求を供給する。

認証依頼送信手段４５は、ローカル通信制御手段４２及びローカル通信手段４１、ＬＡＮ３０、モバイルルータ１０を介して（モバイルルータ１０が、アクセスネットワーク３に接続するモバイルルータアクセス基地局６と通信を行っている場合には、さらに、アクセスネットワーク３及び公衆網１を介して）、ホームネットワーク２上の認証サーバ７に対して、当該認証要求を送信し（ステップＳ６）、認証サーバ７における認証を依頼する。

認証サーバ７では、当該認証要求に係る認証が行われ、下位認証サーバ１２は、その認証結果をＬＡＮ３０、ローカル通信手段４１及びローカル通信制御手段４２を介して、認証結果受信手段４６によって受信する（ステップＳ７）。そして、認証結果受信手段４６で受信した認証結果が、端末１３に接続許可を与えるものであるか否かを判断し（ステップＳ８）、端末１３に接続許可を与えるものである場合には、接続許可を与える端末１３の端末ＩＤを情報格納手段４９内の「認証した利用者の端末ＩＤ」テーブルに格納する（ステップＳ９）。これにより、情報格納手段４９には、接続許可を与える（すなわち、認証に成功した）端末ＩＤ及びユーザＩＤが格納される。

また、認証結果が端末１３に接続許可を与えるものでない場合には、ステップＳ５で「利用者の認証データ」テーブルに格納された利用者の認証データを削除する（ステップＳ１０）。そして、認証結果送信手段４７は、接続の許可／不許可を示す認証結果を端末１３に対して送信する（ステップＳ１１）。

一方、認証要求受付手段４４に供給された外部接続検知結果が、外部接続の利用不可能を示すものである場合には、認証要求受付手段４４から認証データ比較手段４８に認証要求が供給される。そして、認証データ比較手段４８は、情報格納手段４９内の「利用者の認証データ」テーブルから当該端末１３の端末ＩＤに係る認証データを検索し（ステップＳ１３）、当該端末ＩＤに係る認証データが存在するか否かを判断する（ステップＳ１４）。

認証データが存在する場合には、さらに、情報格納手段４９内の「利用者の認証データ」に登録されている認証データと、端末１３から受信した認証データとが一致するか否かを比較し（ステップＳ１５）、両者が一致するか否かを判断する（ステップＳ１６）。両者が一致する場合には、認証結果として端末１３の接続許可を設定し（ステップＳ１７）、両者が一致しなかった場合には、認証結果として端末１３の接続不許可を設定して（ステップＳ１８）、認証結果送信手段４７に対して認証結果を供給する。また、ステップＳ１４で当該端末ＩＤに係る認証データが見つからなかった場合には、認証結果として端末１３の接続不許可を設定して（ステップＳ１９）、認証結果送信手段４７に対して認証結果を供給する。そして、認証結果送信手段４７は、接続の許可／不許可を示すこれらの認証結果を端末１３に対して送信する（ステップＳ１１）。

上記のように、本発明では、端末１３がモバイルルータ下位ネットワーク４上の端末アクセス基地局１１に接続する場合（端末１３がモバイルルータ下位ネットワーク４に参加する場合）、端末１３は、当該端末１３の端末ＩＤ及びこの端末１３の利用者名とパスワードを含む認証データを認証要求として、本発明で新たにモバイルルータ下位ネットワーク４上に配置した下位認証サーバ１２に送信する。

そして、モバイルルータ１０がモバイルルータアクセス基地局５、６

との接続が利用可能である場合、モバイルルータ下位ネットワーク４上の下位認証サーバ１２は、ホームネットワーク２上の認証サーバ７で認証が行われるよう端末１３の認証要求をホームネットワーク２上の認証サーバ７に送信する。そして、ホームネットワーク２の認証サーバ７からの応答である認証結果が認証成功を示すものである場合には、当該端末１３に係る認証データを情報格納手段４９に格納する。下位認証サーバ１２は、このようにして格納した認証データを用いて、次回以降の端末１３の認証を行うことが可能となる。

これによって、例えば、モバイルルータ１０及びモバイルルータ下位ネットワーク４が高速移動をしている場合など、モバイルルータ１０とモバイルルータアクセス基地局５、６との接続が切断しやすい状態にある場合、実際にモバイルルータ１０とモバイルルータアクセス基地局５、６との接続が切断してしまっても、モバイルルータ下位ネットワーク４上の下位認証サーバ１２で認証処理を行うことが可能となる。なお、下位認証サーバ１２は、当該端末を利用する利用者の認証データや当該端末ＩＤを格納している必要がある。したがって、特に、いったん下位認証サーバ１２が属するモバイルルータ下位ネットワーク４に参加したことのある端末１３が、例えば、端末アクセス基地局１１との接続が切れてしまい、モバイルルータ下位ネットワーク４に再び参加しようとする場合などに有効である。

なお、上記の実施の形態では、モバイルルータ１０とモバイルルータアクセス基地局５、６との接続が利用可能か否かに従って、ホームネットワーク２に属する認証サーバ７で認証を行うか、モバイルルータ下位ネットワーク４に属する下位認証サーバ１２で認証を行うかを決定しているが、例えば、全ての端末１３の認証をまず下位認証サーバ１２で行い、認証に失敗した場合のみ、ホームネットワーク２に属する認証サー

バ７に認証の依頼を行うようにすることも可能である。これによって、認証に係る時間や認証サーバ１２へのトラフィックを節約することが可能となる。

また、上記の実施の形態では、下位認証サーバ１２は、認証要求のあった所定の端末から認証要求を受けたタイミングで、所定の端末に係る端末ＩＤや利用者情報のみを情報格納手段４９に格納しているが、あらかじめ全ての認証データを情報格納手段４９に格納しておいたり、任意のタイミングで、下位認証サーバ１２が認証サーバ７から認証データを受信できるようにしたりすることも可能である。

以下、図６を参照しながら、下位認証サーバ１２が、認証サーバ７から、任意のタイミングで認証データを受信できるよう構成された下位認証サーバの内部構成について説明する。図６は、本発明の実施の形態のネットワークに配置されている下位認証サーバの内部構成の別の一例を示すブロック図である。なお、図１に示されている下位認証サーバ１２は、図６に示す内部構成を有している。

図６に示す下位認証サーバ１２は、ローカル通信手段６１、ローカル通信制御手段６２、外部接続検知結果受信手段６３、認証要求受付手段６４、認証データ比較手段６５、認証結果送信手段６６、認証情報複製手段６７、情報格納手段６８により構成される。この図６に示す内部構成と図４に示す内部構成と比較すると、図６に示す下位認証サーバ１２は、ホームネットワーク２上の認証サーバ７における認証結果の処理に係る手段を有さないことに特徴があることがわかる。

また、図６に示す下位認証サーバ１２は、認証情報複製手段６７を有するという特徴がある。この認証情報複製手段６７は、外部接続検知結果受信手段６３から外部接続検知結果を取得し、外部接続が利用可能状況に基づいて、ローカル通信制御手段６２、ローカル通信手段６１、Ｌ

ＡＮ３０、モバイルルータ１０などを介して、ホームネットワーク２上の認証サーバ７から、端末１３の認証に必要な認証データを取得し、取得した認証データを情報格納手段６８に格納することが可能なものである。

これにより、下位認証サーバ１２は、任意のタイミング（ただし、外部接続が利用可能な場合）で、認証サーバ７から、認証に必要となる認証データを取得することが可能となり、このようにして取得した認証データを参照することによって、ホームネットワーク２に属する認証サーバ７と同等の認証能力を発揮できるようになり、認証に係る時間や認証サーバ１２へのトラフィックを節約することが可能となる。なお、例えば、下位認証サーバ１２の情報を、ホームネットワーク２に属する認証サーバ７が格納する情報と同期させるため、例えば一定周期などの所定のタイミングで、認証サーバ７から、認証に必要となる認証データを複製し、情報格納手段６８内の情報を更新することが好ましい。

産業上の利用可能性

以上説明したように、本発明によれば、移動体内に配置されている移動ネットワーク（モバイルルータ下位ネットワーク４）から離れた場所に配置された第１認証サーバ（認証サーバ７）とは別に、第２認証サーバ（下位認証サーバ１２）を移動ネットワーク内に配置し、第２認証サーバにおいても移動端末（端末１３ａ、１３ｂ）の認証が行えるようにするので、移動するモバイルルータと地上側のモバイルルータアクセス基地局との接続が不安定又は不可能な場合でも、移動ネットワークへの接続(参加)を試みている端末の認証を効率良く行うことが可能となる。

請 求 の 範 囲

1. 移動体内に配置されている移動ネットワークに移動端末が参加する場合、前記移動ネットワークから離れた場所に配置された第1認証サーバが、前記移動端末の認証を行うことが可能である端末認証システムにおいて、前記移動ネットワーク内に第2認証サーバを配置し、前記第2認証サーバにおいても前記移動端末の認証が行えるよう構成されていることを特徴とする端末認証システム。

2. 前記第2認証サーバが、前記移動端末の認証を行うことを可能とする認証手段と、前記移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有することを特徴とする請求項1に記載の端末認証システム。

3. 前記移動端末から前記第2認証サーバに対して、認証要求が送信されるよう構成されていることを特徴とする請求項2に記載の端末認証システム。

4. 前記第2認証サーバが、前記第1認証サーバと前記第2認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記第2認証サーバが前記移動端末から前記認証要求を受けた場合、前記第1認証サーバとの通信が可能と判断された場合には、前記第1認証サーバに前記認証要求を送って前記第1認証サーバから前記移動端末の認証結果を受信し、前記第1認証サーバとの通信が不可能と判断された場合には、前記認証手段を用いて前記移動端末の認証を行うよう構成されていることを特徴とする請求項3に記載の端末認証システム。

5. 前記第１認証サーバに前記認証要求を送って前記第１認証サーバから前記移動端末の認証結果を受信した場合、前記第２認証サーバは、前記移動端末の識別情報と前記移動端末の認証結果とを関連付けて、前記情報格納手段に前記認証データとして格納するよう構成されていることを特徴とする請求項４に記載の端末認証システム。

6. 前記第２認証サーバが、前記第１認証サーバと前記第２認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記接続判断手段が前記第１認証サーバとの通信が可能か否かを判断し、前記第１認証サーバとの通信が可能と判断された場合、前記第２認証サーバは、任意のタイミングで前記第１認証サーバから前記移動端末の認証に必要となる前記認証データを取得し、前記情報格納手段に格納するよう構成されていることを特徴とする請求項１に記載の端末認証システム。

7. 前記第２認証サーバは、所定のタイミングで前記第１認証サーバから前記認証データを取得し、前記情報格納手段に格納されている前記認証データを更新するよう構成されていることを特徴とする請求項６に記載の端末認証システム。

8. 前記第２認証サーバで前記移動端末の認証を行って前記移動端末の認証に失敗した場合、前記第２認証サーバは、前記第１認証サーバに前記認証要求を送って前記第１認証サーバから前記移動端末の認証結果を受信するよう構成されていることを特徴とする請求項３に記載の端末認証システム。

9． 前記第２認証サーバから前記認証要求を送信した前記移動端末に対して、前記第１認証サーバ又は前記第２認証サーバで行われた認証結果が通知されるよう構成されていることを特徴とする請求項３に記載の端末認証システム。

10． 移動体内に配置されている移動ネットワークに移動端末が参加する場合、前記移動ネットワークから離れた場所に配置された第１認証サーバが、前記移動端末の認証を行うことが可能である端末認証システムにおける端末認証方法において、前記移動ネットワーク内に配置された第２認証サーバが、前記移動端末の認証を行うことを特徴とする端末認証方法。

11． 前記移動端末が、前記第２認証サーバに対して、認証要求を送信することを特徴とする請求項１０に記載の端末認証方法。

12． 前記第２認証サーバが前記移動端末から前記認証要求を受けた場合、前記第１認証サーバと前記第２認証サーバとの通信が可能か否かを判断し、前記第１認証サーバとの通信が可能と判断された場合には、前記第１認証サーバに前記認証要求を送って前記第１認証サーバから前記移動端末の認証結果を受信し、前記第１認証サーバとの通信が不可能と判断された場合には、前記第２認証サーバが前記移動端末の認証を行うことを特徴とする請求項１１に記載の端末認証方法。

13． 前記第１認証サーバに前記認証要求を送って前記第１認証サーバから前記移動端末の認証結果を受信した場合、前記第２認証サーバは、前記移動端末の識別情報と前記移動端末の認証結果とを関連付けて格納

することを特徴とする請求項１２に記載の端末認証方法。

１４．　前記第２認証サーバが、前記第１認証サーバと前記第２認証サーバとの通信が可能か否かを判断し、前記第１認証サーバとの通信が可能と判断された場合には、任意のタイミングで前記第１認証サーバから前記移動端末の認証に必要となる前記認証データを取得し格納することを特徴とする請求項１１に記載の端末認証方法。

１５．　前記第２認証サーバが、所定のタイミングで前記第１認証サーバから前記認証データを取得し、前記第２認証サーバに格納されている前記認証データを更新することを特徴とする請求項１４に記載の端末認証方法。

１６．　前記第２認証サーバで前記移動端末の認証を行って前記移動端末の認証に失敗した場合に、前記第２認証サーバから前記第１認証サーバに前記認証要求を送り、前記第１認証サーバで認証を行い、前記第１認証サーバから前記第２認証サーバに前記移動端末の認証結果を送信することを特徴とする請求項１１に記載の端末認証方法。

１７．　前記第２認証サーバが、前記認証要求を送信した前記移動端末に対して、前記第１認証サーバ又は前記第２認証サーバで行われた認証結果を通知することを特徴とする請求項１１に記載の端末認証方法。

１８．　移動体内に配置されている移動ネットワークに移動端末が参加する場合、前記移動端末の認証を行うことが可能である端末認証サーバにおいて、前記移動ネットワークから離れた場所に配置された端末認証

サーバとは別に、前記移動ネットワーク内に配置されることを特徴とする端末認証サーバ。

１９．　前記移動端末の認証を行うことを可能とする認証手段と、前記移動端末の認証時に参照する認証データを格納することが可能な情報格納手段とを有することを特徴とする請求項１８に記載の端末認証サーバ。

２０．　前記移動端末から認証要求を受信することを特徴とする請求項１９に記載の端末認証サーバ。

２１．　前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記移動端末から前記認証要求を受けた場合、前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断された場合には、前記移動ネットワークから離れた場所に配置された端末認証サーバに前記認証要求を送って、前記移動ネットワークから離れた場所に配置された端末認証サーバから前記移動端末の認証結果を受信し、前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が不可能と判断された場合には、前記認証手段を用いて前記移動端末の認証を行うことを特徴とする請求項２０に記載の端末認証サーバ。

２２．　前記移動ネットワークから離れた場所に配置された端末認証サーバから前記移動端末の認証結果を受信した場合、前記移動端末の識別情報と前記移動端末の認証結果とを関連付けて、前記情報格納手段に前記認証データとして格納することを特徴とする請求項２１に記載の端末認証サーバ。

２３．　前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能か否かを判断する接続判断手段を有し、前記移動ネットワークから離れた場所に配置された端末認証サーバとの通信が可能と判断された場合、任意のタイミングで、前記移動ネットワークから離れた場所に配置された端末認証サーバから前記移動端末の認証に必要となる前記認証データを取得し、前記情報格納手段に格納することを特徴とする請求項１８に記載の端末認証サーバ。

２４．　所定のタイミングで、前記移動ネットワークから離れた場所に配置された端末認証サーバから前記認証データを取得し、前記情報格納手段に格納されている前記認証データを更新することを特徴とする請求項２３に記載の端末認証サーバ。

２５．　前記認証手段により前記移動端末の認証を行って、前記移動端末の認証に失敗した場合、前記移動ネットワークから離れた場所に配置された端末認証サーバに前記認証要求を送って前記第１認証サーバから前記移動端末の認証結果を受信することを特徴とする請求項１９に記載の端末認証サーバ。

２６．　前記認証要求を送信した前記移動端末に対して、前記移動ネットワークから離れた場所に配置された端末認証サーバ、又は、当該端末認証サーバで行われた認証結果を通知することを特徴とする請求項１９に記載の端末認証サーバ。

FIG. 1

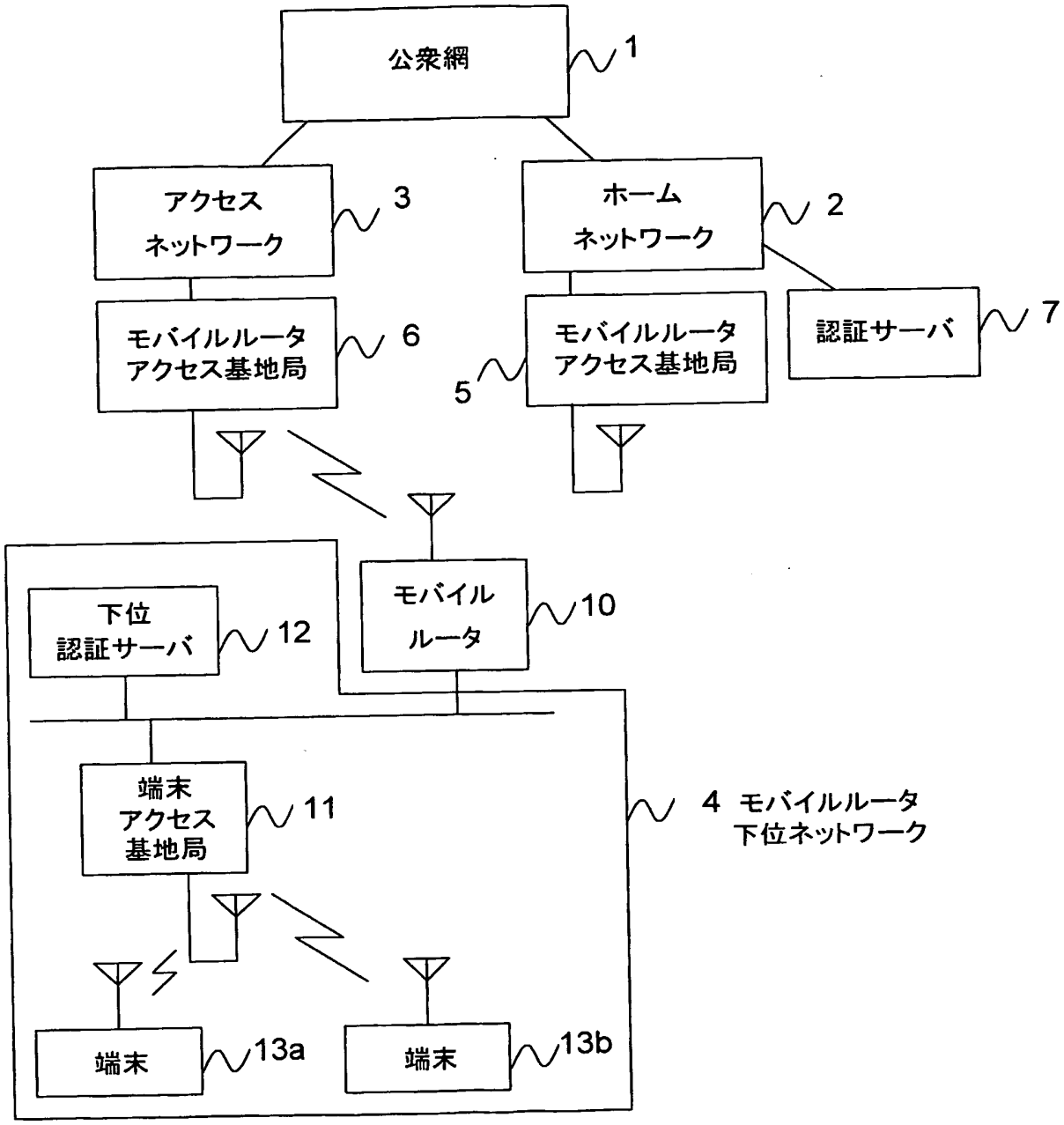

公衆網
1
アクセス
ネットワーク
3
ホーム
ネットワーク
2
モバイルルータ
アクセス基地局
6
モバイルルータ
アクセス基地局
5
認証サーバ
7
下位
認証サーバ
12
モバイル
ルータ
10
端末
アクセス
基地局
11
4 モバイルルータ
下位ネットワーク
端末
13a
端末
13b

FIG. 2

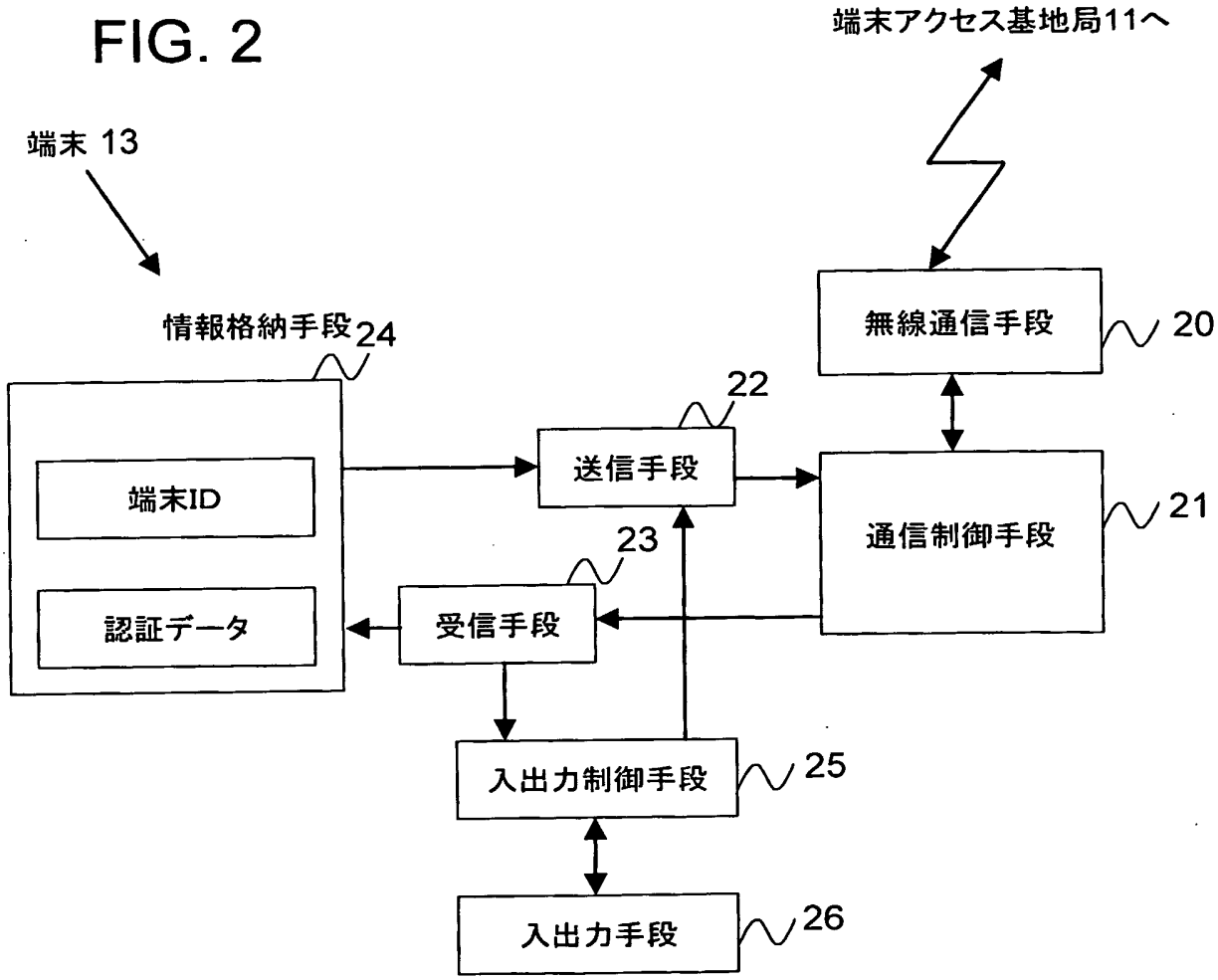

端末アクセス基地局11へ
端末 13
情報格納手段 24
端末ID
認証データ
送信手段
22
受信手段
23
無線通信手段
20
通信制御手段
21
入出力制御手段
25
入出力手段
26

FIG. 3

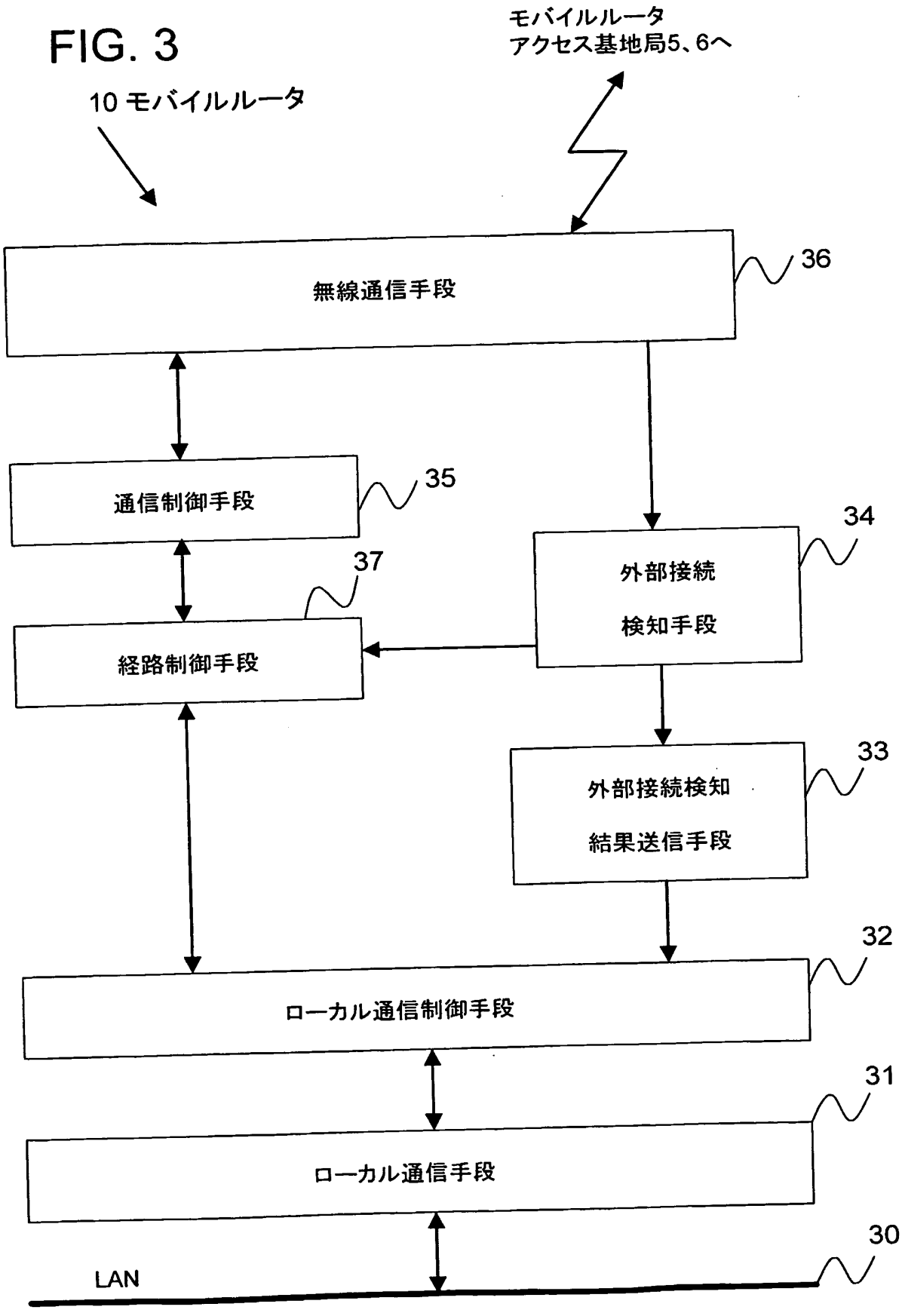

モバイルルータ
アクセス基地局5、6へ
10 モバイルルータ
無線通信手段
36
通信制御手段
35
外部接続
検知手段
34
37
経路制御手段
外部接続検知
結果送信手段
33
ローカル通信制御手段
32
ローカル通信手段
31
LAN
30

FIG. 4

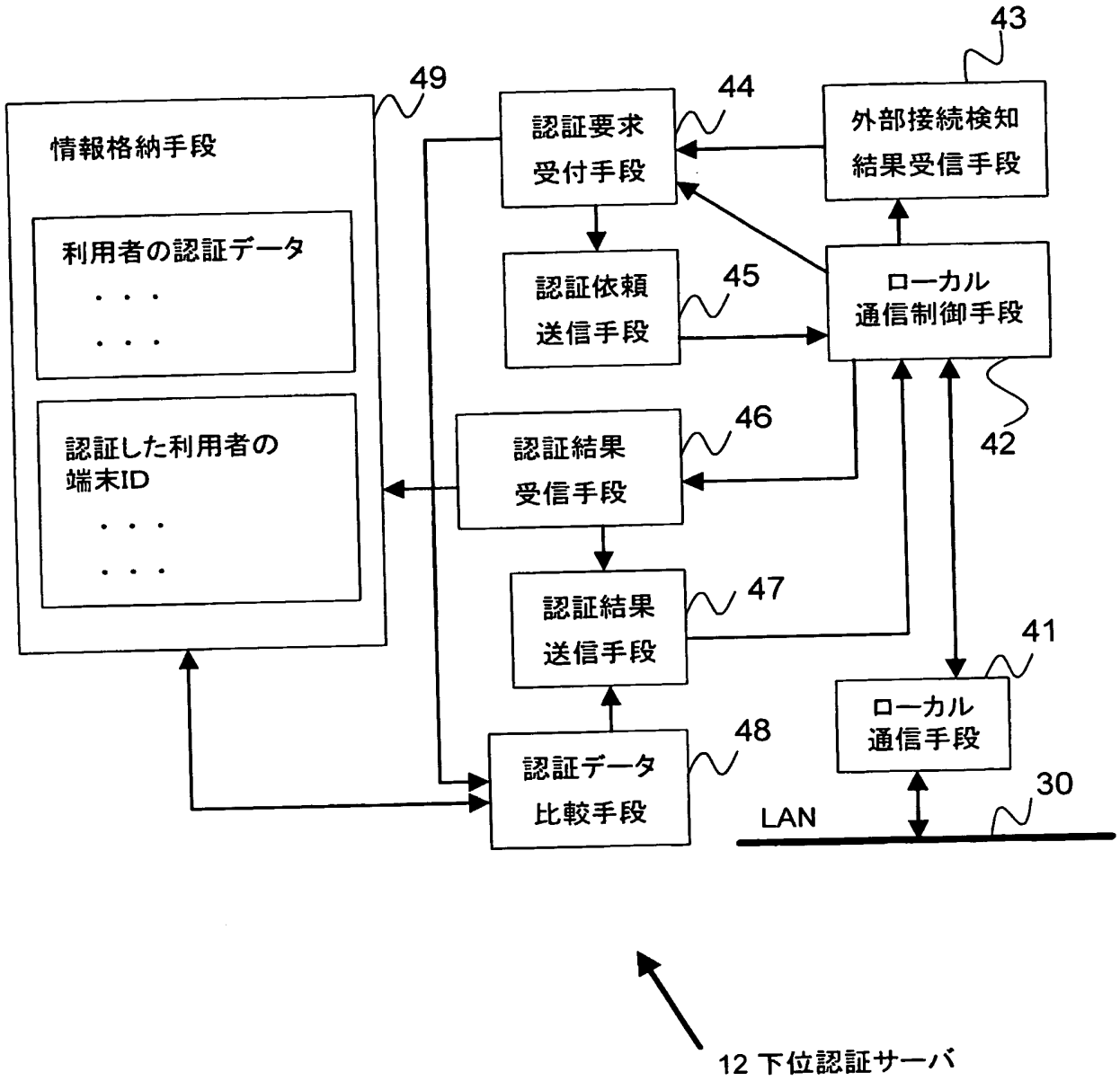

43
49
44
情報格納手段
認証要求
受付手段
外部接続検知
結果受信手段
利用者の認証データ
・・・
・・・
認証依頼
送信手段
45
ローカル
通信制御手段
認証した利用者の
端末ID
・・・
・・・
46
42
認証結果
受信手段
認証結果
送信手段
47
41
ローカル
通信手段
48
認証データ
比較手段
30
LAN
12 下位認証サーバ

FIG. 5

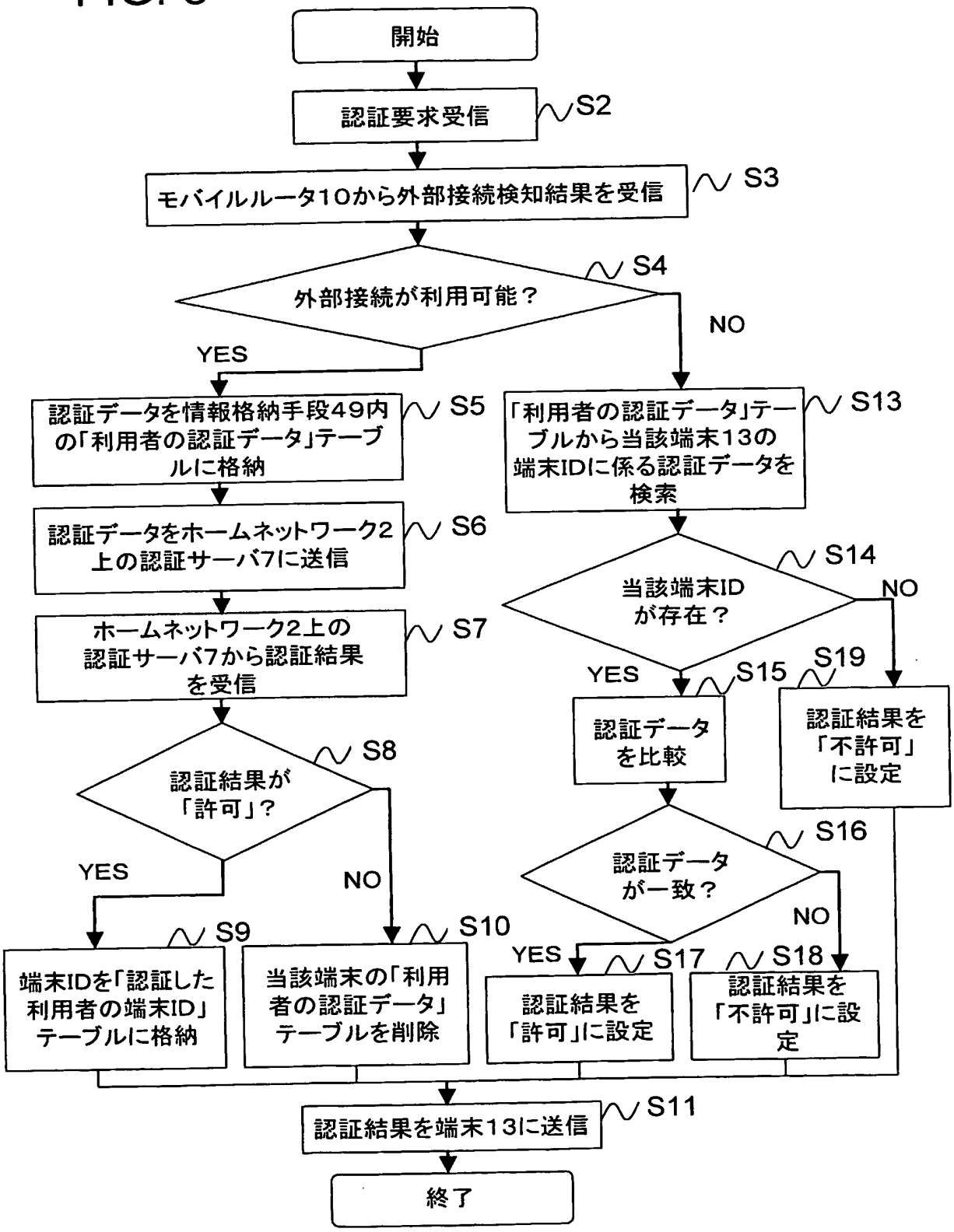
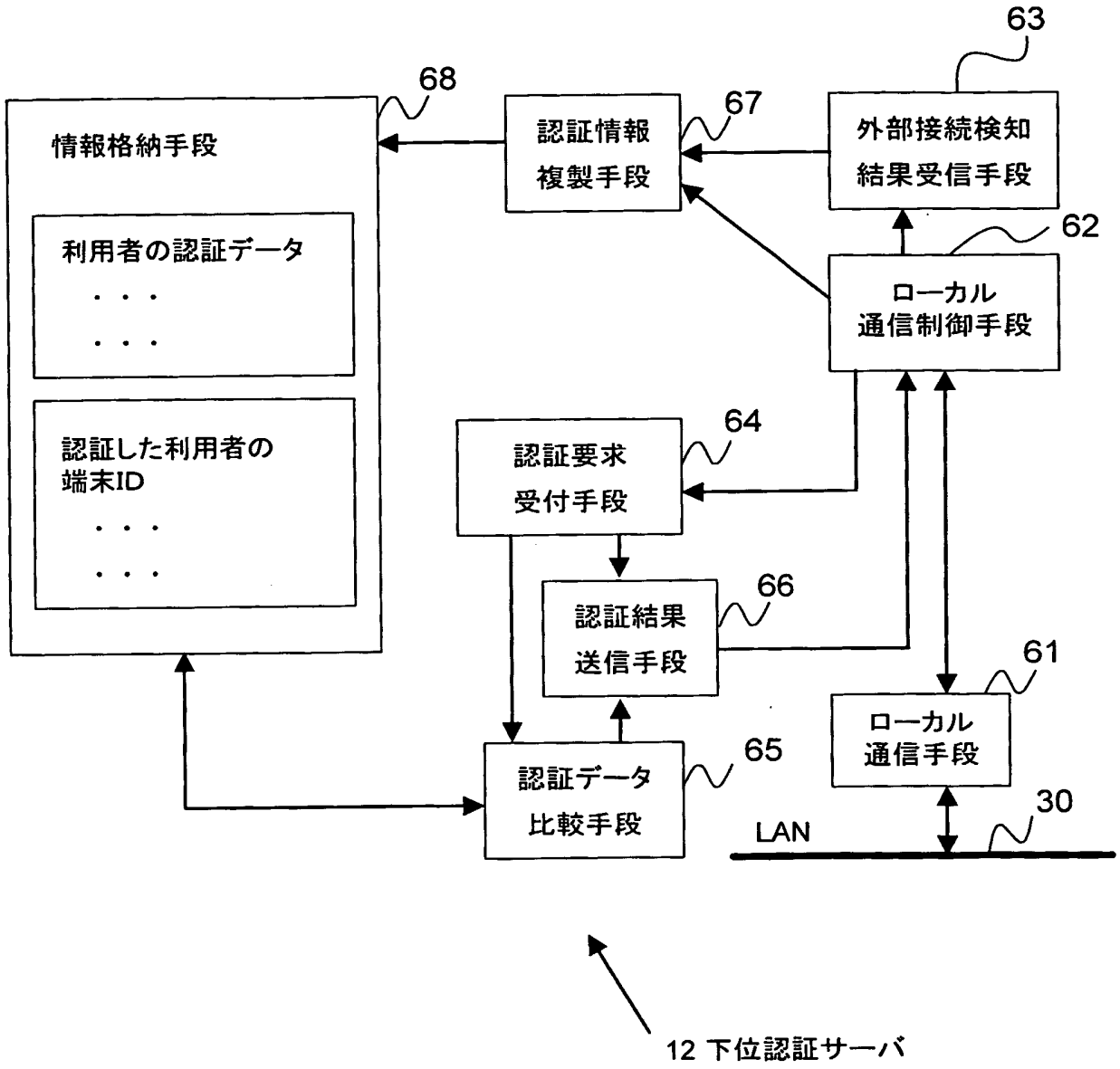

開始
認証要求受信
S2
モバイルルータ10から外部接続検知結果を受信
S3
外部接続が利用可能？
S4
YES
NO
認証データを情報格納手段49内の「利用者の認証データ」テーブルに格納
S5
認証データをホームネットワーク2上の認証サーバ7に送信
S6
ホームネットワーク2上の認証サーバ7から認証結果を受信
S7
認証結果が「許可」？
S8
YES
NO
端末IDを「認証した利用者の端末ID」テーブルに格納
S9
当該端末の「利用者の認証データ」テーブルを削除
S10
「利用者の認証データ」テーブルから当該端末13の端末IDに係る認証データを検索
S13
当該端末IDが存在？
S14
YES
NO
認証データを比較
S15
認証結果を「不許可」に設定
S19
認証データが一致？
S16
YES
NO
認証結果を「許可」に設定
S17
認証結果を「不許可」に設定
S18
認証結果を端末13に送信
S11
終了

FIG. 6


63
68
67
情報格納手段
認証情報
複製手段
外部接続検知
結果受信手段
利用者の認証データ
62
ローカル
通信制御手段
認証した利用者の
端末ID
64
認証要求
受付手段
66
認証結果
送信手段
61
ローカル
通信手段
65
認証データ
比較手段
30
LAN
12 下位認証サーバ